Project	Policies
Document Title	Cloud Solution Provider – Customer Data Access Control & Security Policy

Revision History		
Date	**Version**	**Change**
22/09/2017	1.00	New Document
03/10/2017	1.01	Revision to Annex A
10/10/2017	1.02	Clarification on permission terminology
23/10/2017	QMF Issue 1	Assigned QMF number
26/10/2017	QMF Issue 2	Amended Partner Center Users & added signatory section
20/03/2018	QMF Issue 3	Added scope section, Introduction amended to be concise and moved elements to new sections Lines of Responsibility and Data Access and added statement of consequence for non-adherence. Section Related Documents added
25/04/2018	QMF Issue 4	Addition to Partner Centre Users section
28/08/2020	QMF Issue 5	Updated with new Bytes logo

Contents

Introduction

1. The purpose of this document is to detail the extent to which Bytes Software Services can access Customer data as part of their responsibilities as a Cloud Solution Provider, and to document the controls Bytes has put in place to prevent any unauthorised access.

2. This policy is liable to change on a regular basis. Any changes to the list of Bytes employees with access rights will be detailed in Annex A. Any changes to the extent of Bytes access will be listed in the appropriate section and distributed to Customers.

3. Any employee found to have violated these policies may be subject to disciplinary action as set out elsewhere in the Staff Handbook.

4. This policy is in addition to the responsibilities laid out in other Bytes policies, specifically including but not limited to the Information Security and Data Access policies.

Scope

This policy:

- Encompasses all systems that make up the Microsoft Partner Center provided by Microsoft.
- Only applies to aspects of the Microsoft Partner Center that is managed and controlled by Bytes Software Services.

Related Documents

Please also read:

- Information Security Policy
- Data Breach Procedure
- Data Subject Access Request Procedure
- Data Retention Policy

These documents can be found on the Company's Intranet, on the network under the L:\Library\GDPR drive and on the Bytes website: www.bytes.co.uk .

Policy Details

Lines of Responsibility

Signatories of this policy – must ensure that he or she adheres to the content of this policy and enquire from their Manager clarity on any aspect of this policy that is unclear or needs further explanation.

Managers – Managers are responsible for ensuring that signatories of this policy are aware of and comply with this policy.

EXCO – Oversee that this policy is adhered to by Managers and signatories.

Data Access

1. Customer data is private and belongs to the Customer, it does not belong to Bytes Software Services.

2. Accessing Customer data can only be carried out upon receipt of prior written authorisation from the Customer.

3. The signatory of the Customer providing written authorisation must have the responsibility to do so.

4. The written instruction must contain a clear instruction to access the data.

5. Accessing the Customer's data is only carried out to the extent required to complete the specific task.

6. To ensure the security and integrity of the data it should only be accessed from a Bytes provided Laptop, desktop or Citrix environment.

User Subscription Licenses

Definition

1. This section is concerned with Bytes access to Customer data for User Subscription Licenses (USLs).

2. A USL is a license or collection of pre-defined Microsoft services administered through to Office 365 Admin Centre. This includes but is not limited to the Office 365 Enterprise Plans, Power BI, and Project Online.

Native Access Limitations

1. Bytes manage all Microsoft Cloud Agreements through a Microsoft provided online tool called Microsoft Partner Center which grants a limited ability to see Customer data as described in the Microsoft Cloud Agreement.

2. Partner Center Users with any Agent role will have the ability to view a list of Customers' Azure Active Directory Users

3. Partner Center Users with the Admin Agent or Helpdesk Agent will have the ability to conduct "Admin On Behalf Of" actions on customers' Azure Active Directory (AAD) tenant. This is known as Delegated Admin Permissions (DAP).

4. DAP is the same level of AAD tenant access as a Customer User with the Global Admin role and the same restrictions to data access apply, for example:

    a. Bytes will be unable to directly view User, Group, or Shared Mailboxes
    b. Bytes will be unable to directly view SharePoint data
    c. Bytes will be unable to directly view files in OneDrive for Business

5. Office 365 offers a native Audit Logging feature, allowing Customers to interrogate the system for any changes to configuration or permissions. Where this has not already been enabled, Bytes will (at an appropriate time) automatically activate the Audit Logging feature. Bytes would

strongly encourage Customers to configure configuration, access, and permission change Alerts as part of the Audit Logging functionality.

6. Customers may choose to remove Bytes DAP. This will restrict the ability of Bytes Agents' to assist Customers in any support scenario.

Microsoft Azure

Definition

1. This section is concerned with Bytes access to Customer data for Microsoft Azure

2. Azure is Microsoft's public cloud platform.

3. When a customer orders Azure through the Bytes Microsoft Cloud Agreement, Bytes will provision an empty Subscription or Subscriptions, allowing Customers to provision any Azure Consumption Service.

Native Access Limitations

1. Bytes manage all Microsoft Cloud Agreements through a Microsoft provided online tool called Microsoft Partner Center which grants a limited ability to see Customer data as described in the Microsoft Cloud Agreement.

2. Partner Center Users with the Admin Agent or Helpdesk Agent will have the ability to conduct "Admin On Behalf Of" actions in customers' Azure Subscription(s). This is accomplished by Azure recognising all Agents as a single Foreign User Principal with the Azure Role Based Access Control (RBAC) Owner role. This is an inherited role that cannot be removed by the Customer, Bytes, or Microsoft and is the same role granted to the first User that the Customer specifies.

3. The RBAC Owner role allows the download of most stored data types but Customers can enable native AES 256-bit encryption for all stored data and this is a practice that Bytes would strongly encourage.

4. All actions within an Azure Subscription are automatically tracked using the native Audit Logging tool. This can be used to set alerts for all suspicious activity, a practice that Bytes would strongly encourage.

Additional Controls

Administrative Privileges

1. Bytes operates a Policy of Least Privilege for access to any administrative tool or function, including Partner Center. No member of staff will be granted an Agent role in Partner Center unless their tasks cannot be completed using any other functionality.

2. Access to Partner Center is restricted to Users in Bytes Azure Active Directory.

    a. It is Bytes HR Policy that each employee will have only one entry in the Company Active Directory.
    b. Bytes maintains a general IT Policy of a one-to-one relationship between Active Directory and Azure AD through directory synchronisation, utilising Active Directory Federation Services.

c. The addition of Cloud Only Users in Bytes' Azure AD is reviewed and permitted by the Group Head of IT.
d. Any Azure AD administrative privileges are reviewed and permitted by the Group Head of IT.
e. As an extension of Azure AD administrative privileges any Partner Center roles will be permitted by the Group Head of IT after consultation with Bytes Executive Committee and the Bytes Policy of Least Privilege. A list of these Users can be found at Annex A.
f. Changes to any User's administrative permissions in Azure AD, or Partner Center by extension, can only be completed by a Global Admin on Bytes Azure AD that include members of Bytes Systems Support only.
g. All Bytes employees with access to Partner Center will receive training in confidentiality, and this policy specifically, at appointment. Periodic refresher and update training will also be provided where appropriate.
h. All Bytes employees with access to Partner Center will have their privileges reviewed every six months.

Remote Access

1. Due to the nature of Microsoft Partner Center it can be access from any network, however the security of the network it is being accessed from should be considered. Under no circumstances should public wifi's be used.

Arm's Length Systems

1. Most activities that can be completed on Partner Center have a corresponding API, allowing them to be completed using arm's length tools and systems.

2. Bytes have developed a publicly facing portal allowing Customers to create quotes according to pre-defined Vendor pricelists (including Microsoft), request pricing for non-Tier 1 Vendors, and log & track Licensing Service Desk queries (where this feature has been enabled). Bytes employees also use this portal as part of internal process to raise and complete Customer orders.

3. The Partner Center APIs have been integrated in to the Bytes portal to allow employees to raise quotes, and process orders without any direct access to Partner Center. The APIs used for these tasks do not have any effect on Customer environments other than for generating pricing or provisioning services.

4. For any Partner Center tasks that have not yet had an API released by Microsoft, or where the API has not yet been integrated in to the Bytes portal, only the Bytes employees identified in Annex A will complete the work.

Partner Centre Users

The list of Bytes employees with permissible rights to Partner Center, who have read and agreed to these Terms & Conditions, is maintained by the Sales Operations Director.

See "Annex A" for the current list of Bytes employees with permissible rights to Partner Center.